

# METI's Cyber Security Measures Related to CIIP

Sept. 2004

Shuji Kawaguchi  
Assistant Director, IT Security Policy  
Ministry of Economy, Trade and Industry

# 1. Comprehensive Strategy on Information Security

- METI issued the Comprehensive Strategy on Information Security in October 2003.
- It has three main elements:
  - ✓ Development of self-recoverable social system based on the premise that accidents/incidents in cyber-space often happen,
  - ✓ Public-sector measures that aim to take advantage of “Japan’s high reliability”, and
  - ✓ Action programs for empowerment of the Cabinet Office.

## 2. Simulated Cyber-Attacks on Critical Infrastructure

- The Federation of Electric Power Companies (FEPC), the Central Research Institute of the Electric Power Industry (CRIEPI) and METI will conduct simulated cyber-attacks on the information systems of electric companies from this November.
  
- We plan the following:
  - ✓ Construct a model office network system including interfaces with control systems for electric power plants,
  - ✓ Make scenarios to attack the model system,
  - ✓ Try to access the model system to see whether the interface with the control systems can be reached, according to the scenarios, and
  - ✓ Accumulate expertise to protect electric power infrastructure systems.

- “Vulnerability” refers to a security flaw in a software product, web application, or other item which may affect the confidentiality, integrity, and/or availability of data or services.
- Vulnerability can be used for malicious purposes such as attacks by a computer virus or unauthorized access, which can cause serious damage to the software’s functions or performance.
- METI has built a framework through establishing the official rules for vulnerability handling. (July 7, 2004)
- The vulnerability handling scheme provides vulnerability-related information and suggested countermeasures to the Government, governmental agencies and critical infrastructure sectors preferentially in critical situations.